UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,261	12/31/2003	Ryan Charles Catherman	RPS920030206US2	8466

25299 7590 03/08/2007

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	**PAPER NUMBER**
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,261	CATHERMAN ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 are pending.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1, 12, 14, 17 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 12, 14, 17 of Application No. 10/750,594. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1, 12, 14, and 17 are anticipated by 10/750,594's claims 1, 12, 14, 17 in that the claims 1, 12, 14, and 17 of 10/750,594 contain all of the limitations of the instant application (see Claim-Comparison Table below). Claims 1, 12, 14, and 17 of the instant application therefore are not patentably

distinct from 10/750,594's claims and as such are unpatentable for obvious-type double patenting (*In re Goodman (CAFC) 29 USPQ2d 2010 (12/31/1993)*).

Claim	Application No. 10/749,261	Claim	Application No. 10/750,594
1	A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising: generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable; creating a non-public, signing key pair that is injected into a plurality of valid devices; verifying at a credential server that an endorsement key of a requesting device is a	1	A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising: generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable; creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server; verifying by utilizing said non-public, secure value that an endorsement

	valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is		key of said valid device is a valid endorsement key of said endorsement key pair that was generated during manufactured of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server; and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment

	confirmed having been generated from within a valid device.		manufacturer) of the device.
12	A data processing system comprising: a processor; a trusted platform module (TPM) chip; a bus for interconnecting said processor and said TPM chip; a network interface with communication means for connecting said TPM to a secure credential server; and means whereby said TPM is able to verify an endorsement key pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the	12	A data processing system comprising: a processor; a trusted platform module (TPM) chip; a bus for interconnecting said processor and said TPM chip; a network interface with communication means for connecting said TPM to a secure credential server; and means, whereby said TPM is able to verify an endorsement key pair as being a valid pair generated within said TPM by utilizing a secure, private, single-use value inserted by a TPM vendor into the TPM during

	TPM during manufacture of the TPM.		manufacture of the TPM.
14	A data processing system utilized for issuing endorsement certificates, comprising: a processor; a memory couple to said processor via an interconnect; a security mechanism for ensuring optimum security of processes within said data processing system; input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and secure communication	14	A data processing system utilized for issuing endorsement certificates, comprising: a processor; a memory couple to said processor via an interconnect; a security mechanism for ensuring optimum security of processes within said data processing system; input/output mechanism for receiving a first value received from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and secure communication means for receiving an

	means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key; and program means for determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices.		endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key and a second value provided for verifying that said EK was generated from within one of said manufactured TPM devices; and program means for determining, by utilizing said second value, when said EK is a valid EK of an endorsement key pair that was generated within one of said manufactured TPM devices.
17	A system for securely creating an endorsement certificate for a TPM device in an insecure	17	A system for securely creating an endorsement certificate for a device in an insecure

	environment, said system comprising: means for generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable; means for creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server; means for verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid		environment, said system comprising: means for generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable; means for creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server; means for verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during

	device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device.		manufacture of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server; and means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device wherein said inserting is completed only when said verifying step is confirmed.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 1-6, 8-22, 24, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener (US 2002/0169717) in view of Smith et al. (US 6,233,685).

Regarding claim 1:

Challener discloses generating for a valid device an endorsement key pair that includes a private key and a public key (paragraphs 0022-0024, public key, P2, and private key, P4), wherein said private key is not public readable (inherent trait of public/private key pairs); creating a non-public, signing key pair (paragraph 0021 and 0024, endorsement key with public key, P1, and private key, P3) [Examiner interprets non-public key pair in light of the specification as a key pair that is used amongst a few select entities or only temporarily in the communication.] ; and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device (paragraph 0024, certificate, C2) only when said endorsement key is confirmed having been generated from within a valid device (it is common in the art and inherent that the key is generated within the device (see US 6,973,191 for reference)). Challener does not disclose verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (inherent property of identity based authentication of a CA to contain information about the key pair). Smith et al. discloses in columns 8 lines 35-67 to column 9 lines 1-28, verifying at a credential server (Certificate Authority, CA) a signature of said endorsement key

(device key as used in Smith et al.) is a public signing key (authorities public key) of signing key pair.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method of Challener for generating an endorsement key, creating a signing key, and inserting an endorsement certificate with the method of Smith et al. for verifying that a key is in fact a key from the device in order to certify the device (Smith et al, column 8 lines 60-63).

Claim 2:

Smith et al. discloses providing a signing key certificate for said signing key pair, said signing key certificate including a public singing key of said signing key pair; and forwarding said signing key certificate via a secure communication medium to said credential server (column 9 lines 12-17, the device presents the certificate and the information contained in it (it is inherent to include the public key of the certificate with the certificate) to the requesting party (CA)).

Claim 3:

Challener al. discloses signing said public key of the endorsement key pair (paragraph 0023, the public key, P2, and the certificate, C1, are sent to the CA (it is inherent to send information encrypted by the public key of the certificate along with the certificate)) with a public signing key (P1) of said signing key pair when creating the endorsement key (EK); and forwarding a resulting signed EK to said credential server to initiate a credential process (paragraph 0023).

Claim 4:

Challener discloses receiving said signed EK at said credential server (paragraph 0023); comparing the public signing key within the signing key certificate with a signature from the signed EK (it is inherent to use the public key of the certificate); and when the public signing key matches the signature, confirming (verifying) said EK as originating from a valid device (paragraph 0023).

Claim 5:

Challener discloses a CA which inherently stores the credential in a database of said credential server; monitors for a request from a customer to provide said certificate to said device (this is done with the request for certification); and following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device (this is done after the certification).

Claim 6:

It is inherent in TCPA for the endorsement key to be once writable, public readable (see TCPA Spec 1.1b, page 261) therefore it would have been obvious to one of ordinary skill in the art to make the certificate once writable, public readable.

Claim 8:

Smith et al. discloses that the CA can be a remotely located third party with a secure connection (column 8 lines 31-43).

Claim 9:

The endorsement key is a unique key per platform module. It would have been obvious to one of ordinary skill in the art at the time of invention to make the signing key a unique key per platform module.

Claims 10 and 11 teach the system associated with the method disclosed in claim 1.

Claims 12 and 13:

Challener discloses a processor (Figure 1, 110), a TPM chip (111), a bus for interconnecting said processor and said TPM chip (it is inherent to connect two or more components through a bus), a network interface with communication means for connecting said TPM to a secure credential server (Communications Adapter 134 and Network 160). The means whereby said TPM is able to verify an endorsement key pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture of the TPM, means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed EK, and means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate as the system of the method claims 1-5, rejected under the same arguments.

Claim 14 and 15:

Claims 14 and 15 disclose the functionality and system of a Certificate Authority. It is inherent for a Certificate Authority to have a processor, a memory coupled to said processor, a security mechanism, input/output mechanism, secure communication means, and program means for determining if data is authentic.

Claims 17-22, 24, and 25 correspond to the system of method claims 1-6, 8, and 9. Claims 17-22, 24, and 25 are rejected under the same logic as claims 1-6, 8, and 9.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the TCPA compliant chipset of Challener with the method and system for certifying information of Smith et al. in order to increase security of initial device certification (Smith et al, column 8 lines 56-60).

Claims 7 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener and Smith et al. as applied to claims 1 and 17 above, and further in view of Wood et al. (US 2006/0072747).

Challener and Smith et al. discloses the method and system of claims 1 and 17 respectively, but they do not disclose a temporary key. Wood et al. discloses using a temporary key (figure 6, step 605-645) after which the key is no longer used (discarded). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method and system of claims 1 and 17 disclosed by Challener and Smith et al. with the temporary key of Wood et al. in order to provide additional security (Wood et al, paragraph 0039).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses TCPA compliant chipsets and certificate generation and exchange.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

Taghi T. Arani
Primary Examiner
3/5/07